Copy to D.D(CSA)
DSD 10.
Sigs. 6
DDY.
Sigs. 5 12/8

15(I)

TOP SECRET

TICOM/I-66

Paper by Dr. OTTO BUGGISCH of

OKH/In.7/VI and OKW/Chi on TYPEX.

Attached is the translation of a write-up done at Revin in August 1945 by Dr. Buggisch on what he remembers of OKH research on the Typex Machine.

TICOM
12 August 1945

No. of pages 3

Distribution:-

British
Director
D.D.3
D.D.4
D.D.(N.S.)
D.D.(M.W.)
D.D.(A.S.)
A.D.(C.C.R)(2)
Lt.Col. Leathem

TICOM
Chairman
S.A.C.(2)
Cdr. Bacon
Cdr. MacKenzie
Cdr. Tandy
Lt.Col. Johnson
Lt.Col. Lewis Powell
Lt.Cdr. Manson
Major G.W. Morgan
Major Seaman
Capt. Cowan
Lt. Fehl
Lt. Vance
Ticom Files (2)

U.S.
OP 20-G (2) (via Lt. Pendergrass)
G-2 (via Lt.Col. Hilles)
S.S.A. (2) (via Major Seaman)
Director, S.I.D. USFET
(via Lt.Col. Johnson)

Additional
Mr. Twinn
Mr. Alexander
S.A.C. for D.S.D.10.Admiralty
Signals 6. War Office
D.D.Y. War Office
Signals 5. Air Ministry

State of research into the English Cipher Machine Type X at OKH/IN 7/VI.

In January or February, 1942, in view of my being engaged on Enigma, the file on Type X was also made available to me at my department OKH/In 7/VI. This contained various reports on investigations. The first of them by Insp. (?) Breede probably written in the Winter of 39/40; but they contained complete nonsense. An imaginary machine which had nothing whatever to do with Type X was described in them. The only important things were later investigations by some mathematicians from the first half of 1940. I do not know who the people were, as the reports as a rule did not bear the names of the authors, but were only signed off by the Head of Section. But I seem to remember hearing that Dr. Schulz was one of the leading personalities. Now, after three and a half years, I still remember the following:-

1) By means of ordinary letter statistics on some 10,000 cipher letters, it was established that this was a system similar to Enigma; i.e. a system in which any letter X of the alphabet was changed, on an average equally frequently, into each of the other letters a, b, ..., except X itself. The frequency-curve of the cipher letters which one would expect theoretically was fairly well attained - Z, it is true, being assumed to be the separating letter. In this connection, I remember the following curious phenomenon, which, however, had no practical significance: the statistics of all the first, all the second, and all the third letters of the cipher text produced the result that in the clear text A must be especially frequent in the first position, I in the second, and R in the third; this was obviously caused by the fact that AIR was a particularly frequent beginning of a message.

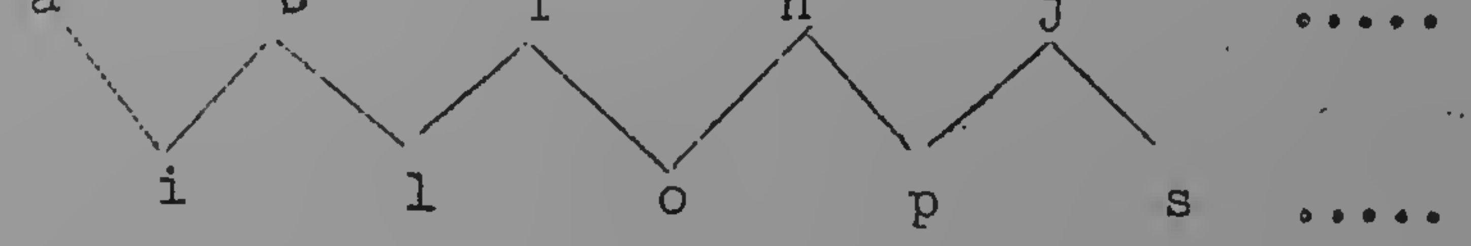
2) The examination of a few thousand of the 5-letter message settings showed that in the case of one message being enciphered immediately after another, the following relationship between the two message-settings frequently existed:

a) In the case of messages enciphered one immediately after the other, the two right-hand letters very often remained unchanged.

b) The 3 left-hand letters often changed, when passing from the first message to the second, in the same way as the initial position of the wheels of a German Army Enigma would change after a message of the same length had been enciphered, with the following two differences:

A) The centre and thus also the left-hand wheel moves more quickly; and it was possible to explain this greater speed exactly by assuming that there were 2, instead of 1, turn-overs on the right-hand wheel.

B) The sequence of the letters on the circumference of the wheels could not be purely alphabetical: it must have been conditionally alphabetical - I believe roughly as follows:



It is worthy of note that the findings a) and b) were achieved entirely without the aid of captured material or other knowledge of the machine, and only developed out of a very large volume of traffic, and based solely on the fact that when encyphering a message the operator very often chose exactly, or very nearly, the final position of the previous message as the new message setting.

3) A Type X without wheels was captured during the French campaign (probably near Dunkirk), and also some documents in which an English cipher security officer points out that he has recently noticed frequent breaches of the strict regulation that wheels should be turned on at random after a message has been enciphered. It was particularly dangerous in the case of the two wheels which did not turn on automatically if they remained in the same position in 2 consecutively enciphered messages, for this gave the enemy important hints on the construction of the machine. In addition the wiring of a reflector wheel was captured somewhere.

4) I vaguely remember reading somewhere in the papers something about 25 wheels belonging to the machine.

5) Casual consideration was also given to the question whether, if one knew the inner wiring of the wheels, one might be able to tackle the problem of breaking. But nobody at In 7/VI went into this in any detail as, in view of the fact that we had no wheel wirings at all, it was of no practical interest.

At any rate, no single Type X message was broken while I was at IN 7/VI (later Ag N/NA), i.e. until June '44, and I cannot believe that this changed at all in the following months. I have also never heard of any other department engaged on cryptanalysis ever decoding a Type X message.

(trans: K.C.K.)